EXHIBIT E

Trials@uspto.gov
Tel: 571-272-7822

Paper 25
Date: November 4, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

MPH TECHNOLOGIES OY,
Patent Owner.

IPR2019-00824
Patent 9,712,502 B2

Before SALLY C. MEDLEY, KAMRAN JIVANI, and JOHN D. HAMANN, *Administrative Patent Judges*.

HAMANN, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining Some Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

In this *inter partes* review, instituted pursuant to 35 U.S.C. § 314, Apple Inc. ("Petitioner") challenges the patentability of claims 1–10 ("the challenged claims") of U.S. Patent No. 9,712,502 B2 (Ex. 2002, "the '502 patent"), owned by MPH Technologies Oy ("Patent Owner"). We have jurisdiction under 35 U.S.C § 6. This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

For the reasons discussed herein, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–6 and 10 are unpatentable, but Petitioner has not shown by a preponderance of the evidence that claims 7–9 are unpatentable.

II. BACKGROUND

A. Procedural History

Petitioner filed a Petition requesting *inter partes* review of the challenged claims of the '502 patent. Paper 2 ("Pet."). The Petition is supported by the Declaration of David Goldschlag, Ph.D. (Ex. 1002). Patent Owner filed a Preliminary Response. Paper 6 ("Prelim. Resp.").

We instituted *inter partes* review of all of the challenged claims of the '502 patent on all of the grounds raised in the Petition. Paper 7 ("Dec. on Inst."), 6–7, 34. Patent Owner filed a Response to the Petition. Paper 13 ("PO Resp."). The Response is supported by the Declaration of Professor George N. Rouskas, Ph.D. (Ex. 2003) and the Declaration of Michael S. Borella (Ex. 2010). Petitioner filed a Reply to Patent Owner's Response. Paper 16 ("Pet. Reply"). The Reply is supported by an additional Declaration of David Goldschlag, Ph.D. (Ex. 1022). Patent Owner filed a Sur-Reply to Petitioner's Reply. Paper 23 ("PO Sur-Reply").

An oral hearing was held on August 11, 2020. A transcript of the oral hearing is included in the record. Paper 24 ("Tr.").

B. Related Matter

The parties identify *MPH Techs. Oy v. Apple Inc.*, Case No. 4:18-cv-05935-PJH (N.D. Cal.), as a matter that may affect or would be affected by a decision in this proceeding. Pet. 2; Paper 4, 1. The parties also identify as related matters the following *inter partes* reviews: IPR2019-00822, IPR2019-00823, IPR2019-00825, and IPR2019-00826, which involve the parties and patents related to the '502 patent. Pet. 2; Paper 4, 1.

C. The Challenged Patent (Ex. 2002)

The '502 patent relates to the "secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network." Ex. 2002, 6:38–41. According to the '502 patent, "[a]n essential idea of [its] invention is to use the standard [Internet Protocol ('IP') Security ('IPSec')] protocol . . . between the intermediate computer and the second computer and an 'enhanced IPSec protocol' between the first computer and the intermediate computer." *Id.* at 7:38–41, 1:54. More specifically, the '502 patent states that "[t]he advantage of [its] invention is that [a] logical IPSec connection shared by the first and the second computer can be enhanced by the first and the intermediate computer without involvement of the second computer." *Id.* at 10:38–41. The '502 patent adds: "[i]n particular[,] the so-called 'ingress filtering' performed by some routers [(e.g., the second computer)] does not pose any problems when translations of addresses are used." *Id.* at 10:41–44.

Figure 1, shown below, "illustrates an example of a telecommunication network of the invention" of the '502 patent. *Id.* at 9:55–56.

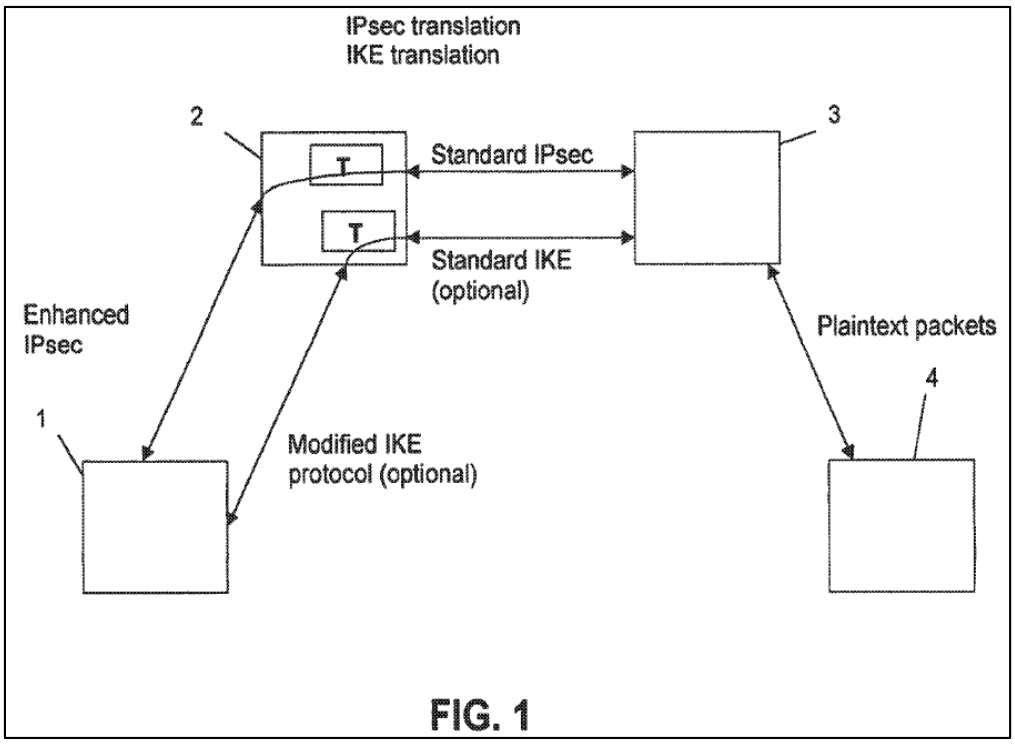


FIG. 1

Figure 1 shows an example of a telecommunication network in accordance with the invention of the '502 patent. *Id.* at 10:4–5. As illustrated, the network comprises: (i) a first computer (client computer 1) that is served by (ii) an intermediate computer (server 2), and (iii) host computer 4 that is served by (iv) a second computer (security gateway 3). *Id.* at 10:4–9. Security gateway 3 "supports the standard IPSec protocol," while client computer 1 and server 2 support an enhanced IPSec protocol. *Id.* at 10:9–12. The '502 patent discloses that the first computer (i.e., client computer 1) in Figure 1 is a mobile terminal. *Id.* at 11:5–7, 11:13–14.

"In the example of F[igure] 1, an IPSec connection is formed between . . . client computer 1 (the first computer) and . . . security gateway 3 (the second computer)." *Id.* at 10:46–48. The '502 patent discloses that

"[m]essages to be sent to . . . host terminal 4 from . . . client computer 1 are first sent to . . . server 2, wherein an IPSec translation[, *inter alia*,] . . . takes place." *Id.* at 10:60–62. Put differently, "[w]hen the intermediate computer receives the packet sent . . ., it performs an address and [Security Parameters Index ('SPI')] translation, ensuring that the security gateway (host 3 of F[igure] 1) can accept the packet." *Id.* at 12:1–4, 2:40–41. The '502 patent states that "translation[s can be] . . . performed[, for example,] by means of a translation table stored at the intermediate computer[,with t]he outer IP header address fields and/or the SPI-values [being] changed by the intermediate computer so that the message can be forwarded to the second computer." *Id.* at 7:46–50.

According to the '502 patent, "[m]ost of the packet is secured using IPSec, . . . [but] the intermediate computer . . . is able to use the outer IP addresses and the incoming SPI value to determine how to modify the outer address and the SPI to suite the second computer, which is the next destination." *Id.* at 12:1–11. "[T]he confidentiality of the packets is not compromised, . . . [because t]he intermediate computer does not know the cryptographic keys used to encrypt and/or authenticate the packets, and can thus not reveal their contents," according to the '502 patent. *Id.* at 10:32–37. After translation, "the message can be sent to . . . security gateway 3, which sends the message further in plain text to . . . host terminal 4." *Id.* at 10:62–64.

D. The Challenged Claims

Petitioner challenges claims 1–10 of the '502 patent, of which claim 1 is the sole independent claim. Claim 1 is illustrative of the challenged claims and is reproduced below:

> 1. A computer for sending secure messages, and for enabling secure forwarding of messages in a telecommunication network by an intermediate computer to a recipient computer, comprising:
>
> a computer configured to connect to a telecommunication network;
>
> the computer configured to be assigned with a network address in the telecommunication network, wherein the computer is a mobile computer in that the address of the mobile computer changes;
>
> the computer configured to form a secure message by encrypting the data payload of a message and giving the message a unique identity and a destination address of an intermediate computer, wherein the unique identity and the destination address are capable of being used by the intermediate computer to find an address to a recipient computer;
>
> the computer configured to send the secure message to the intermediate computer for forwarding of the encrypted data payload to the recipient computer; and
>
> the computer configured to set up a secure connection using a key exchange protocol.

Ex. 2002, 22:41–62.

E. Instituted Grounds of Unpatentability

We instituted trial based on the following grounds of unpatentability, which are all the grounds of unpatentability raised in the Petition:

	References	35 U.S.C. §[1]	Challenged Claims
1.	Request for Comments 3104 ("RFC3104"),[2] Grabelsky[3]	103(a)	1–9
2.	RFC3104, Grabelsky, Wagner[4]	103(a)	10

Pet. 20–58.

III. LEVEL OF ORDINARY SKILL IN THE ART

To determine whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). In assessing the level of ordinary skill in the art, various factors may be considered, including the "type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field." *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995)

---

[1] The Leahy-Smith America Invents Act ("AIA") included revisions to 35 U.S.C. § 103 that became effective on March 16, 2013. Because the '502 patent issued from an application having an effective filing date before March 16, 2013, we apply the pre-AIA version of the statutory basis for unpatentability.

[2] G. Montenegro & M. Borella, *RSIP Support for End-to-end IPsec*, Request for Comments 3104, The Internet Society (Oct. 2001) ("RFC3104") (Ex. 1004).

[3] U.S. Patent No. 7,032,242 B1 (issued Apr. 18, 2006) (Ex. 1006).

[4] David Wagner & Bruce Schneier, *Analysis of the SSL 3.0 Protocol*, Proc. 2d USENIX Workshop on Elec. Com. (Nov. 1996) ("Wagner") (Ex. 1007).

(citing *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986)). "[O]ne or more factors may predominate." *Id.*

In our Decision on Institution, we adopted Petitioner's proposed definition for one having ordinary skill in the art at the time of the invention of the '502 patent as one who would have had "a bachelor's (B.S.) degree in Computer Science, Computer Engineering, Electrical Engineering, or an equivalent field, as well as at least 2–5 years of academic or industry experience in the field of Internet security." Dec. on Inst. 7–8 (citing Pet. 17; Ex. 1002 ¶¶ 31–32). Patent Owner does not dispute our adoption of Petitioner's definition, nor otherwise address the level of ordinary skill at the time of the invention of the '502 patent. *See generally* PO Resp.; *see also* Ex. 2003 ¶ 22.

Because Petitioner's definition of the level of skill in the art is consistent with the '502 patent and the asserted prior art, we maintain Petitioner's definition for purposes of this Final Written Decision. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *GPAC*, 57 F.3d at 1579; *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978). We apply Petitioner's definition in our analysis below.

IV. CLAIM CONSTRUCTION

Because the Petition was filed after November 13, 2018, we construe the challenged claims by applying "the standard used in federal courts, in other words, the claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b), which is articulated in *Phillips* [*v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc)]." *See* Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340,

51,343, 51,358 (Oct. 11, 2018) (amending 37 C.F.R. § 42.100(b) effective November 13, 2018) (now codified at 37 C.F.R. § 42.100(b) (2019)). Under *Phillips*, the words of a claim are generally given their "ordinary and customary meaning," which is the meaning they would have to a person of ordinary skill in the art at the time of the invention, in light of the specification and prosecution history. *See Phillips*, 415 F.3d at 1312–13.

Petitioner identifies for construction the terms "secure connection" and "unique identity," as recited in claim 1. Pet. 18–20. Patent Owner identifies for construction the term "mobile computer," as recited in claim 1. PO Resp. 11–17. We address these three terms below.

A. Secure Connection and Unique Identity

In the Petition, Petitioner argues that (i) "'*secure connection*' should be construed to encompass 'one or more security associations,'" and (ii) "'*unique identity*' should be construed as 'one or more parameters that uniquely identify a secure connection.'" Pet. 18–19. In our Decision on Institution, "we conclude[d] that no express claim construction of the terms 'secure connection' or 'unique identity' [was] necessary" because in its Preliminary Response "Patent Owner [did] not argue that RFC3104 or Grabelsky fails to disclose these terms and, therefore, these terms are not in controversy." Dec. on Inst. 9 (citations omitted). In the subsequent papers, the parties confirm that there is no reason to construe these terms because "Patent Owner does not dispute that the primary reference involves a secure connection," and "does not dispute that some form of a unique identity is found in the primary reference." PO Resp. 18, 23; *see also* Pet. Reply 8 (agreeing that we need not construe these terms). Accordingly, we find that no express constructions of "secure connection" or "unique identity" are

needed. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)) ("[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'").

B. Mobile Computer

Patent Owner argues that "the term 'mobile computer' in the claims means 'a computer that moves from one network to another as opposed to a computer that is only capable of a static secure connection.'" PO Resp. 11. Patent Owner adds that a mobile computer "must be moving between networks," and that "[m]erely being *capable of* moving is insufficient." PO Sur-Reply 5. Petitioner argues that "[t]o the extent the Board determines this term needs to be construed" it means "a computer that is capable of moving between networks or physical locations." Pet. Reply 2.

We address the parties' arguments below as they relate to (i) the claim language, (ii) the '502 patent's Specification, and (iii) the extrinsic evidence.

1. Claim Language

a. Claim 1's Language

Patent Owner argues that claim 1 recites a "'mobile computer' in a specific context." PO Sur-Reply 4. To that end, Patent Owner argues that claim 1 recites:

> "A computer for sending secure messages, and for enabling secure forwarding of messages . . . by an intermediate computer to a recipient computer," including:
>
> - "the computer configured to be assigned with a network address in the telecommunication network, wherein the computer is *a mobile computer* in that the address of the mobile computer changes"

- "the [mobile] computer configured to send the secure message to the intermediate computer for forwarding of the encrypted data payload to the recipient computer"

PO Resp. 11–12 (quoting Ex. 2002, 22:41–62) (emphasis added). In its Sur-Reply, Patent Owner quotes and paraphrases additional language from claim 1, namely that:

> the computer is [a] "mobile computer in that the address of the mobile computer changes" and where [the] mobile computer forms the secure message to have an encrypted data payload and "a unique identity and a destination address of an intermediate computer," and where the mobile computer sends the secure message to the intermediate computer which uses the unique identity and destination address formed by the mobile computer to determine a final destination address to enable the secure "forwarding of the encrypted data payload to the recipient computer" by the intermediate computer.

PO Sur-Reply 4–5 (quoting and citing Ex. 2002, 22:41–62). Patent Owner argues that "[i]t is not enough that the computer be capable of moving between networks in some other context at some other time," and that the computer "must be moving between networks in the recited context" of claim 1. *Id.* at 5.

We disagree with Patent Owner that the language of claim 1 supports its proposed construction. Nothing in claim 1 relates to a mobile computer actually moving between networks. Ex. 2002, 22:41–62. Rather, claim 1 focuses on the operations of a "computer for sending secure messages, and for enabling secure forwarding of messages in a telecommunication network by an intermediate computer to a recipient computer," wherein the computer is a mobile computer. *Id.* at 22:41–44 (reciting claim 1's preamble). Each of claim 1's limitations begins with "the computer configured to," followed by specific operations (i.e., "connect," "be assigned," "form," "send," and

"set up") that concern sending secure messages and enabling secure forwarding of the messages. *Id.* at 22:45–62. In the context of claim 1, the mobile computer forms the secure message (i.e., "encrypting the data payload of a message and giving the message a unique identity and a destination address of an intermediate computer"), and sends the secure message to an intermediate computer for forwarding to a recipient computer. *Id.* Claim 1 does not recite that the mobile computer moves between networks. *Id.* To the contrary, claim 1 recites that "the computer is a mobile computer *in that* the address of the mobile computer changes." *Id.* at 22:48–50 (emphasis added). In other words, claim 1 describes what a mobile computer is (i.e., it can change addresses, or put differently, is capable of moving between networks), not that it must move between networks in the context of claim 1. *Id.* Our conclusion is further supported by the additional limitation in claim 1 that "the computer [is] configured to set up a secure connection using a key exchange protocol." *Id.* at 22:61–62. As we discuss below, setting up a secure connection using a key exchange protocol is consistent with the mobile computer being at a point of attachment, rather than moving between networks. *See infra* Section IV(B)(2)(c) (discussing the Specification teaching that the mobile terminal must establish a new IPSec connection from each point of attachment, and using the IKE key exchange). Accordingly, claim 1's language does not support Patent Owner's construction.

b. Claim 7's Language

Claim 7 depends from claim 1, and recites "wherein the computer is configured to send a signaling message to the intermediate computer *when the computer changes its address* such that the intermediate computer can

know that the address of the computer is changed." Ex. 2002, 23:11–15 (emphasis added). In our Decision on Institution, we noted that in its Preliminary Response, Patent Owner did not address the impact, if any, of dependent claim 7's claim language on the construction Patent Owner proposed for this term at that time. Dec. on Inst. 11. Thereafter, in its Response, Patent Owner addresses claim 7 with respect to its new proposed construction for this term. PO Resp. 12–13.

Patent Owner argues that "[c]laim 7 is consistent with [its] proposed construction." *Id.* at 12. In particular, Patent Owner argues that "[c]laim 7 recites a specific configuration of the invention where a signaling message is sent from the mobile computer to the intermediate computer to provide its new IP address when the mobile computer has changed networks." *Id.* According to Patent Owner, one of ordinary skill in the art "would readily recognize that there are other ways by which mobility could be provided in claim 1 using different operations different from those in claim 7." *Id.*

We disagree with Patent Owner that claim 7 is consistent with its proposed construction for this term. Rather, claim 7 adds additional functionality to the mobile computer (i.e., "send a signaling message") for use "*when the computer changes its address*." Ex. 2002, 23:11–15 (emphasis added). In other words, claim 7 adds functionality to claim 1 for "when" the mobile computer changes addresses (in other words, moves from one network to another). *Id.* Rather than supporting Patent Owner's proposed construction, the language of claim 7 supports Petitioner's proposed construction that a mobile computer "is capable of moving between networks" because claim 7's additional functionality at least suggests that this functionality (including mobile computer movement) is not

present in claim 1, which is broader than dependent claim 7. *See Phillips*, 415 F.3d at 1315 ("[T]he presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim."); *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 910 (Fed. Cir. 2004) ("[W]here the limitation that is sought to be 'read into' an independent claim already appears in a dependent claim, the doctrine of claim differentiation is at its strongest.") (citation omitted). Moreover, we do not find that Patent Owner's arguments, which we discuss below, concerning the Specification's disclosure overcome this presumption.

2. Specification

a. Patent Owner's Arguments

Patent Owner argues that the '502 patent's Specification "describes 'mobility' in the background section" in a way that "is consistent with the understanding that a 'mobile computer' at least moves from one network to another." PO Resp. 13 (citing Ex. 2002, 4:35–39). More specifically, Patent Owner argues that the Specification states that "[i]n this text, the term mobility and mobile terminal does not only mean physical mobility, instead the term mobility is in the first hand meant moving from one network to another, which can be performed by a physically fixed terminal as well." *Id.* (quoting Ex. 2002, 4:35–39); PO Sur-Reply 2–3. Patent Owner argues that the plain import of this sentence "is that a requirement of mobility is that the computer is 'moving from one network to another.'" PO Sur-Reply 3.

In addition, Patent Owner argues that "the Background of the Invention [section of the '502 patent] criticizes systems where the host computer is only capable of a static or fixed connection." PO Resp. 14

(citing Ex. 2002, 4:17–28, 4:40–46, 4:61–64). Put differently, Patent Owner argues that "[t]he background section of the ['']502 [p]atent consistently disparages secure connection systems where the computer is not moving from one network to another and instead are capable of only static secure connections." PO Sur-Reply 3 (citing PO Resp. 14–15 (citing Ex. 2003 ¶ 77; Ex. 2002, 4:17–28, 4:40–46, 4:61–64)); *see also* PO Resp. 14–16 (citing same). Patent Owner argues that "[t]hus, the mobile computer is explicitly described as one that is not fixed to a static secure connection (its home address) but is instead moving between networks." PO Sur-Reply 3. Patent Owner argues that this is confirmed by the '502 patent's disclosure that "[t]he mobile terminal is mobile in the sense that it changes its network point of attachment frequently." *Id.* at 4 (quoting Ex. 2002, 4:51–52).

In addition, Patent Owner argues that "the Detailed Description of the invention [section] describes mobile computers as being devices that are **not** limited to a static or fixed connection." PO Resp. 15. In support of this argument, Patent Owner block quotes from the Detailed Description section of the '502 patent, without further explanation. *Id.* at 15–17 (quoting Ex. 2002, 7:56–8:7, 11:5–29). The quoted passages generally disclose, *inter alia*, that a first computer (e.g., a mobile computer) can send a signal (e.g., a registration request) to an intermediate computer so that address fields in a translation table can be modified to account for the change of addresses for enabling mobility. *See* Ex. 2002, 7:56–8:7, 11:5–29. Patent Owner then argues that "[t]hus, the mobile computer 1 in Figure 1 of the patent is described as *maintaining* an IPSec connection through second computer 3 by modifying the endpoint of the IPSec connection as the mobile computer changes addresses." *Id.* at 17 (annotating Ex. 2002, Fig. 1) (emphasis

added). Similarly, Patent Owner argued, during the oral hearing, that a computer "is functioning as a mobile computer insofar [as] it is moving from one network to another and maintaining, *the key is that it's maintaining the same secure connection*" — "it's moved from one network to another and ha[s] a different address, but it doesn't have to establish a new secure connection." Tr. 49:14–19 (emphasis added).

In addition, Patent Owner argues that its proposed construction is consistent with the '502 "patent's stated purpose: to securely forward a secure message when a computer is mobile, rather than merely when it is fixed to a certain network." PO Sur-Reply 5 (citing Ex. 2002, 4:17–38, 7:51–60).

Lastly, Patent Owner discounts Petitioner's reliance on the background section's discussion of a mobile terminal and a mobile host allegedly forming static secure connections, and instead Patent Owner argues that its proposed construction "is informed by fundamental aspects of the [S]pecification," namely (i) that "the background section of the ['']502 [p]atent consistently disparages secure connections where the mobile device is confined to a static secure connection," and (ii) "the detailed description section of the ['']502 [p]atent consistently describes a mobile computer as moving from one network to another and thereby is not limited to a static secure connection." *Id.* at 5–6.

b. Petitioner's Arguments

Petitioner argues that Patent Owner's proposed construction is "an improper and overly narrow construction of the term 'mobile computer,' which attempts to import numerous additional requirements into this basic term." Pet. Reply 1. More specifically, Petitioner argues that Patent

Owner's proposed construction "imports essentially the same additional requirements into the claims that the Board already rejected at institution, namely that the 'mobile computer' must be able to move *while maintaining its secure connection*." *Id.* at 2 (citing Dec. on Inst. 11).

Petitioner also argues that the Specification refers to "mobile terminal" and "mobile host" as "computers that only establish a 'static secure connection.'" *Id.* at 5–6. For example, Petitioner argues that the Specification discloses that because "IPSec connections are bound to fixed addresses, the mobile terminal must establish a new IPSec connection from each point of attachment." *Id.* at 6 (citing PO Resp. 15 (quoting Ex. 2002, 4:61–64)) (emphases omitted). For another example, Petitioner argues that the Specification states that "IPSec is intended to work with static network topology, where hosts are fixed to certain subnetworks," and "[i]f IPSec is used with a ***mobile host***, the IKE key exchange *will have to be redone from every new visited network*." *Id.* (citing PO Resp. 1 (quoting Ex. 2002, 4:17–28)). Petitioner argues that "this passage plainly uses the term 'mobile host' in conjunction with a computer reestablishing static IPSec connections when moving rather than maintaining them." *Id.* (citing Ex. 1022 ¶ 15).

c. Our Analysis

We disagree with Patent Owner that the cited portions of the Specification support its proposed construction for this term. First, we find

that Patent Owner conflates "mobility" with "mobile computer."[5] The Specification states that "the term *mobility* . . . meant moving from one network to another," rather than the term "mobile computer" having this meaning. Ex. 2002, 4:35–39 (emphasis added). Moreover, the Specification uses the term "mobility" as a capability or condition. For example, the Specification uses the term "mobility" as follows: (i) certain "protocols are not well suited to *mobility*"; (ii) "[t]he intermediate host might be a Mobile IP home agent, that provides *mobility* for the connection between the mobile terminal and the home agent"; (iii) a disclosed "method solves the *mobility* problem, at the cost of adding extra headers to packets"; and (iv) "[o]ne example of a change in the [security association ('SA')] between the first computer and the intermediate computer is the change of addresses for enabling *mobility*." Ex. 2002, 5:8–9, 5:18–22, 5:33–34, 7:56–58 (emphases added). In other words, mobility is a capability a mobile computer has, rather than being synonymous with mobile computer. As such, these passages from the Specification support Petitioner's construction that a mobile computer is "a computer that is capable of moving between networks," rather than Patent Owner's construction requiring that a "mobile computer must be moving between networks."

---

[5] Patent Owner likewise argues that we concluded in our Decision on Institution that a "'mobile computer' must at least be 'moving from one network to another.'" PO Sur-Reply 3 (quoting Dec. on Inst. 10). This is incorrect. Instead, we found "that the '502 patent teaches that *mobility* 'mean[s] moving from one network to another.'" Dec. on Inst. 10 (quoting Ex. 2002, 4:35–37) (emphasis added). We also expressly stated that we did not reach "whether 'a computer that is capable of moving from one network to another' differs from the plain meaning of 'mobile computer,' as this [was] not in controversy" at the institution stage. *Id.* at 10–11.

Second, we are not persuaded by Patent Owner's arguments that the '502 patent's background section criticizes and disparages systems where the host computers are only capable of a static or fixed connection. PO Resp. 14–15. These host computers are not mobile computers, but rather "are fixed to certain subnetworks." Ex. 2002, 4:18–20. Put differently, for these hosts "when an IPSec tunnel has been formed by using Internet Key Exchange (IKE) protocol, the tunnel endpoints are fixed and remain constant." *Id.* at 4:20–23. In contrast, a mobile computer has the capability to move between networks (i.e., can change its network point of attachment frequently). *Id.* at 4:51–52 ("The mobile terminal is mobile in the sense that it changes its network point of attachment frequently."). The Specification makes clear that a mobile computer is capable of moving between networks (as opposed to requiring such movement), even if it would have to "establish a new IPSec connection from each point of attachment," or put differently, "the IKE key exchange *will have to be redone from every new visited network*." *Id.* at 4:23–25, 4:61–64 (emphasis added). Hence, Patent Owner's construction also is incorrect to the extent that the latter portion (i.e., "as opposed to a computer that is only capable of a static secure connection") would exclude a mobile computer from establishing a secure connection (static or otherwise) from each point of attachment. Ex. 2002, 4:51–52, 4:61–64.

Third, we find that Patent Owner's proposed construction is unworkable as to when such alleged movement needs to have occurred. Patent Owner agrees that "[c]ertainly the computer is at times going to be connected to a given network because it establishes a secure connection with a given network." Tr. 49:12–14. Despite this, Patent Owner argues that the

proper construction for this term requires that a mobile computer must be moving between networks. *E.g.*, *id.* at 49:14–16. However, whether or not the mobile computer has changed its point of attachment and established a new IPSec connection before sending a secure message to the intermediate computer is immaterial to claim 1's limitations. Ex. 2002, 4:17–25, 4:61–64, 22:40–62. Again, the mobile computer in claim 1 simply sends a secure message to the intermediate computer from a point of attachment to the network — no movement is required. *Id.* at 22:40–62. Again, claim 1 is focused on the mobile computer forming the secure message (i.e., "encrypting the data payload of a message and giving the message a unique identity and a destination address of an intermediate computer"), and sending the secure message to an intermediate computer for forwarding to a recipient computer. *Id.*

Fourth, we are not persuaded by Patent Owner's argument that its proposed construction is consistent with the '502 patent's "stated purpose." PO Sur-Reply 5. The portions of the Specification that Patent Owner cites do not purport any "stated purpose," but rather relate to additional functionality to handle, *inter alia*, addressing when a mobile computer moves networks. Ex. 2002, 4:17–38, 7:51–60. This functionality is implicated in claim 7, but not claim 1. *Compare id.* at 22:40–62, *with id.* at 23:11–15; *see also Helmsderfer v. Bobrick Washroom Equip., Inc.*, 527 F.3d 1379, 1383 (Fed. Cir. 2008) ("It is often the case that different claims are directed to and cover different disclosed embodiments."). We also note that the '502 patent's Abstract does not relate to mobility, but instead relates to the subject matter of claim 1, including that the first computer forms a secure message by giving the message a unique identity and a destination

address, and that the message is sent from the first computer to the intermediate computer after which the destination address and the unique identity are used to find an address to the second computer. Ex. 2002, code (57).

Fifth, we find inapposite Patent Owner's arguments that a mobile computer moves from one network to another, *maintaining the same secure connection*.[6] *E.g.*, PO Resp. 17; Tr. 49:14–19. Simply put, maintaining the same secure connection is not part of Patent Owner's proposed construction. PO Resp. 11. Nor is it warranted by the claim language or Specification, as we discuss above. *See supra*. The '502 patent's Specification clearly describes the concept of a mobile terminal having the capability to move between networks (and establish secure connections while at a network). *E.g.*, Ex. 2002, 4:23–25, 4:35–39, 4:51–53. The Specification also provides additional disclosed functionality to handle addressing for a secure connection when a mobile terminal moves. Ex. 2002, 7:56–8:7. It is this additional functionality (such as recited in claim 7) that Patent Owner cites from the detailed description section of the '502 patent, but there is no justification in the intrinsic evidence to import these additional features into the term "mobile computer." *See Baran v. Medical Device Techs.*, 616 F.3d 1309, 1316 (Fed. Cir. 2010) ("It is not necessary that each claim read on every embodiment."); *Helmsderfer*, 527 F.3d at 1383. "It is long-settled that

[6] Patent Owner's proposed construction for "mobile computer" from its Preliminary Response was "a computer that is capable of moving from one network to another while maintaining a connection." Prelim. Resp. 4. We did not adopt that proposed construction. Dec. on Inst. 10–11. Patent Owner's new proposed construction does not include "while maintaining a connection." PO Resp. 11.

even though 'claims must be read in light of the specification of which they are a part, it is improper to read limitations from the written description into a claim.'" *Bradium Techs. LLC v. Iancu*, 923 F.3d 1032, 1049 (Fed. Cir. 2019) (quoting *Wenger Mfg., Inc. v. Coating Mach. Sys., Inc.*, 239 F.3d 1225, 1237 (Fed. Cir. 2001)).

Lastly, we find that Patent Owner raised for the first time during the oral hearing the issue of disavowal of claim scope for the term "mobile computer," and cited to cases that were nowhere in the papers. Tr. 53:6–55:16. A new argument may not be raised during the oral hearing because Petitioner has no effective opportunity to review the argument and respond. *See* Patent Trial and Appeal Board Consolidated Trial Practice Guide 85 ("Consolidated Practice Guide") (Nov. 2019) (available at https://www.uspto.gov/TrialPracticeGuideConsolidated) ("During an oral hearing, a party may rely upon appropriate demonstrative exhibits as well as evidence that has been previously submitted in the proceeding, but may only present arguments relied upon in the papers previously submitted."); *see also Dell Inc. v. Acceleron, LLC*, 884 F.3d 1364, 1369 (Fed. Cir. 2018) (holding that the Board was not obligated to consider an "untimely argument . . . raised for the first time during oral argument"); Paper 8 (Scheduling Order), 7 ("Patent Owner is cautioned that any arguments not raised in the response may be deemed waived."). Accordingly, we do not consider this argument.

3. Extrinsic Evidence

The parties cite to declarations of their experts in support of their proposed constructions. *E.g.*, PO Resp. 17 (citing Ex. 2003 ¶¶ 72–80); Pet. Reply 3–8 (citing Ex. 1022 ¶¶ 7–15); PO Sur-Reply 3–10. Likewise, the

parties cite to the deposition testimony of the parties' experts to argue for their proposed constructions. *See generally* PO Resp.; Pet. Reply; PO Sur-Reply.

We reviewed the cited expert testimony, and we find it of little help. "Although expert testimony and declarations are useful to confirm that the construed meaning is consistent with the denotation ascribed by those in the field of the art . . . such extrinsic evidence cannot be used to vary the plain language of the patent document." *Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1332 (Fed. Cir. 2003) (citing *Pitney Bowes, Inc. v. Hewlett–Packard Co.*, 182 F.3d 1298, 1309 (Fed. Cir. 1999) & *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1584 (Fed. Cir. 1996)). As we discuss above, we find that the intrinsic evidence provides that the plain and ordinary meaning of "mobile computer" to one of ordinary skill in the art, in view of the Specification, covers a computer that is capable of moving between networks. *See Supra* Section IV(B)(1)–(2). Accordingly, to the extent that the experts' testimony is contrary to this conclusion, we give it no weight. *See Phillips*, 415 F.3d at 1318 (stating that "a court should discount any expert testimony 'that is clearly at odds with the claim construction mandated by the claims themselves, the written description, and the prosecution history, in other words, with the written record of the patent.'") (citation omitted).

Lastly, we note that the dictionary definition for "mobile" offered by Petitioner's expert, Dr. Goldschlag, is consistent with the meaning of mobile computer provided by the intrinsic evidence. Ex. 1022 ¶ 9. Namely,

Merriam-Webster[7] defines "mobile" as "capable of moving or being moved." *Id.* (quoting Ex. 1025, 797).

In summary, we have reviewed the parties' submitted extrinsic evidence, but we give it little weight in light of the clear language of the intrinsic evidence. *See Wi-LAN, Inc. v. Apple Inc.*, 811 F.3d 455, 462 (Fed. Cir. 2016) (finding extrinsic evidence "is generally of less significance than the intrinsic record" in matters of claim construction); *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1583 (Fed. Cir. 1996) (finding that when "an analysis of the intrinsic evidence alone will resolve any ambiguity in a disputed claim term[,] . . . it is improper to rely on extrinsic evidence").

4. Summary

Based on our review of the parties' arguments and the evidence of record, we agree with Petitioner[8] and conclude that "mobile computer" covers "a computer that is capable of moving between networks."

V. PRINCIPLES OF LAW

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time of the invention to a person having ordinary skill in the art. *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis

[7] Merriam-Webster's Collegiate Dictionary, Eleventh Edition (2003).
[8] Petitioner's proposed construction for this term is "a computer that is capable of moving between networks *or physical locations*." Pet. Reply 2 (emphasis added). To resolve the parties' disputes, we need not, and thus do not, reach whether being capable of moving between physical locations should be included within the meaning of mobile computer. *See Nidec*, 868 F.3d at 1017.

of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of non-obviousness, if present.[9] *See Graham*, 383 U.S. at 17–18. When evaluating a claim for obviousness, we also must "determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

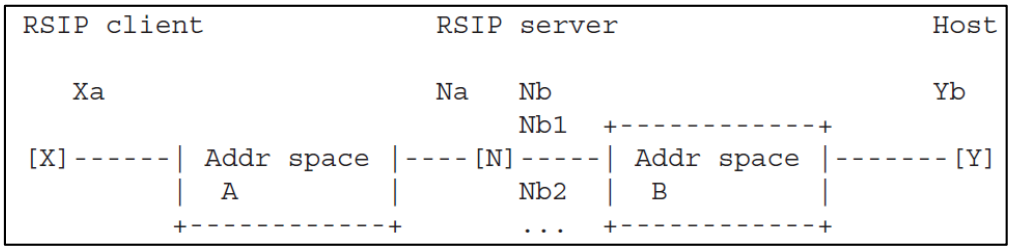
VI. ALLEGED OBVIOUSNESS OVER RFC3104 AND GRABELSKY

Petitioner argues that the combination of RFC3104 and Grabelsky renders claims 1–9 of the '502 patent obvious under 35 U.S.C. § 103(a). Pet. 20–54. We have reviewed the parties' arguments and the evidence of record. For the reasons that follow, we determine that Petitioner (1) shows by a preponderance of the evidence that claims 1–6 would have been obvious to one of ordinary skill in the art in view of RFC3104 and Grabelsky; and (2) does not show by a preponderance of the evidence that claims 7–9 would have been obvious to one of ordinary skill in the art in view of RFC3104 and Grabelsky.

A. Summary of RFC3104

RFC3104 "proposes mechanisms to handle," and "specifies RSIP extensions to enable," end-to-end IPSec. Ex. 1004, 1–2. A figure, shown below, appearing on page 2 of RFC3104 illustrates a "model" topology, in accordance with RFC3104's teachings. *Id.* at 2.

[9] Patent Owner does not present arguments or evidence of such objective evidence of non-obviousness in its Response. *See generally* PO Resp.



RFC3104 provides the above illustrated "model" topology "[f]or clarity" in discussing its teachings. *Id.* As shown, "[h]osts X and Y belong to different address spaces A and B, respectively, and N is an [intermediate] RSIP server." *Id.* at 3. RFC3104 teaches that "N has two addresses: Na on address space A, and Nb on address space B. For example, A could be a private address space, and B the public address space of the general Internet." *Id.*

RFC3104 enables "RSIP client X to initiate . . . IP[S]ec sessions to a legacy . . . IP[S]ec node Y." *Id.* at 3. To that end, RFC3104 teaches that "RSIP client X and server N must arrive at an SPI value to denote the incoming IP[S]ec security association from Y to X." *Id.* at 5. RFC3104 adds: "Once N and X make sure that the SPI is unique within both of their SPI spaces, X communicates its value to Y as part of the IP[S]ec [SA] . . . establishment process." *Id.* According to RFC3104, "[t]his ensures that Y sends IP[S]ec packets . . . to X via address Nb using the negotiated SPI." *Id.* In such a scenario, "IP[S]ec packets from Y destined for X arrive at RSIP server N." *Id.* "RSIP server N . . . examin[es the] packet[s] sent by Y, destined for X[, which] . . . implies that 'source' refers to Y and 'destination' refers to Y's peer, namely, X's presence at N." *Id.* at 3. N demultiplexes each of the IPSec packets "based on the following minimum tuple of demultiplexing fields:" protocol, SPI, and destination IP address. *Id.* at 5. RFC3104 teaches that "[i]f N is able to find a matching mapping, it tunnels

the packet to X according to the tunneling mode in effect." *Id.* Otherwise, RFC3104 teaches that "N . . . MUST discard the packet." *Id.*

B. Summary of Grabelsky

Grabelsky relates to allowing IPSec "to be used with distributed network address translation . . . by mapping a local . . . [IP] address of a given local network device and a IP[S]ec . . . [SPI] associated with an inbound IP[S]sec [SA] . . . that terminates at the local network device." Ex. 1006, code (57). "A router allocates locally unique security values that are used as the IP[S]ec SPIs." *Id.* Figure 21, shown below, "is a block diagram illustrating a SPI-to-internal network address table layout." *Id.* at 6:13–14.

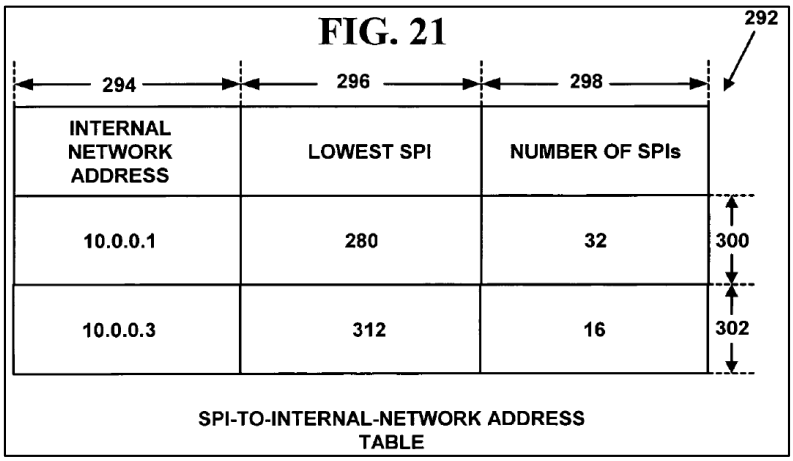


Figure 21, shown above, illustrates "a SPI-to-internal network address table," in accordance with Grabelsky's teachings. *Id.* at 27:56–57. Grabelsky teaches that "a network address for [a] first network device is stored with . . . one or more locally unique security values in a table [(e.g., the table of Figure 21)] associated with [a] second network device." *Id.* at 27:21–24, 27:56–58. Grabelsky teaches that "[t]he table is used to maintain a mapping between a network device and a locally unique security value for distributed network address translation with security." *Id.* at 27:24–27.

In accordance with Grabelsky's teachings, for incoming packets using IPSec, the router (which routes data packets to another external computer network) maintains a mapping between local IP addresses of network devices and SPI values. *Id.* at 6:34–35, 32:32–34. Grabelsky teaches that when an IPSec packet arrives on the router, the router examines a SPI value in the IPSec packet's outermost header, which is typically visible. *Id.* at 32:35–39. "The SPI value in the IP[S]ec header is used to determine a local IP address of a destination network device," according to Grabelsky's teachings. *Id.* at 32:39–41.

C. Challenged Claim 1

1. Undisputed Limitations

a. Computer for Sending Secure Messages

Petitioner argues that RFC3104 discloses "[a] computer for sending secure messages, and for enabling secure forwarding of messages in a telecommunication network by an intermediate computer to a recipient computer," as recited in claim 1's preamble. Pet. 29–30. More specifically, Petitioner argues that "RFC3104 discloses sending a message (e.g., data packets) from a host Y ('*computer*') to a host X ('*recipient computer*') via an RSIP server N ('*intermediate computer*')." *Id.* at 29 (citing Ex. 1004, 2; Ex. 1002 ¶ 86). Petitioner argues that "[t]he interconnected computer configuration allowing host Y to communicate with host X via RSIP server N represents a '*telecommunication network*' as recited in the claims." *Id.* (citing Ex. 1002 ¶ 87). Petitioner also argues that "[a]n IPSec [SA] . . . is established from Y to X." *Id.* at 30 (citing Ex. 1004, 5). According to Petitioner, "[o]nce an SA is established, host Y is able to securely send

messages to RSIP client X, forwarded through RSIP server N." *Id.* (citing Ex. 1004, 5; Ex. 1002 ¶ 89).

b. Connect to a Telecommunication Network

Petitioner argues that RFC3104 teaches "a computer [that is] configured to connect to a telecommunication network," as recited in claim 1. *Id.* at 31. More specifically, Petitioner argues that "the mechanisms described in RFC3104 are used within telecommunications networks, for example, private networks and public networks such as the 'Internet.'" *Id.* (citing Ex. 1004, 3; Ex. 1002 ¶ 90). "Both hosts X and Y are connected to the telecommunications network, having network addresses that enable them to exchange secure messages," according to Petitioner. *Id.* (citing Ex. 1004, 3; Ex. 1002 ¶ 90).

c. Assigned with a Network Address

Petitioner argues that RFC3104 discloses that "the computer [is] configured to be assigned with a network address in the telecommunication network," as recited in claim 1. *Id.* at 31–32. More specifically, Petitioner argues that RFC3104 discloses that hosts X and Y "belong to different address spaces A and B, respectively, and N is an RSIP server. N has two addresses: Na on address space A, and Nb on address space B. For example, A could be a private address space, and B the public address space of the general Internet." *Id.* (citing Ex. 1004, 3; Ex. 1002 ¶ 91).

d. Form a Secure Message

Petitioner argues that RFC3104 discloses that "the computer [is] configured to form a secure message by encrypting the data payload of a message and giving the message a unique identity and a destination address of an intermediate computer," as recited in claim 1. *Id.* at 34–42. Petitioner

argues that one of ordinary skill in the art "would have understood that the data payload of the packet sent from Y to X would be encrypted before being sent from Y." *Id.* at 34 (citing Ex. 1002 ¶ 95). More specifically, Petitioner argues that RFC3104 discloses that an IPSec SA is established from Y to X. *Id.* (citing Ex. 1004, 5). In addition, Petitioner argues that one of ordinary skill in the art "would have understood that in accordance with IPSec standards, the data payload of the packet would be encrypted in order to protect confidentiality of the data." *Id.* at 35 (citing Ex. 1002 ¶¶ 96–97).

Petitioner argues that RFC3104 teaches that "the packet sent from Y to X includes a '*destination address*' of the host N (i.e.[,] *an intermediate computer*)," as "the message is first sent from Y to N, and then from N to X." *Id.* (citing Ex. 1004, 3, 5; Ex. 1002 ¶ 99). According to Petitioner, one of ordinary skill in the art "would have understood that in order to send a packet to X via RSIP server N (as detailed in RFC3104), the packet would first require a destination address of RSIP server N, namely address 'Nb on address space B,' in order to be properly routed to RSIP server N." *Id.* at 36 (citing Ex. 1004, 3; Ex. 1002 ¶ 100). "RFC3104 further confirms this, stating that 'Y sends IPsec packets (protocols 51 and 50 for AH and ESP, respectively) . . . to X *via address Nb* using the negotiated SPI,'" according to Petitioner. *Id.* (citing Ex. 1004, 5).

Petitioner argues that the combination of RFC3104 and Grabelsky teaches giving the message a unique identity. *Id.* More specifically, Petitioner argues that RFC3104 and Grabelsky teach "packet headers (i.e., the IP header and IPSec protocol header) of a packet received by RSIP server N from host Y, which contain a set of 'demultiplexing fields' including an SPI value." *Id.* (citing Ex. 1004, 5). "The SPI value, the set of

'demultiplexing fields,' and the packet headers, each provide a '*unique identity*,'" according to Petitioner. *Id.* (citing Ex. 1002 ¶ 101); *see also id.* at 36–42 (citing Ex. 1004, 5; Ex. 1006, 20:49–50, 20:63–66, 21:33–37, 22:17–18, 23:5–9, 24:5–8, 24:21–28, Figs. 15–18; Ex. 1002 ¶¶ 102–105, 107–108, 111–112) (arguing that the message has a unique identity). According to Petitioner, one of ordinary skill in the art would have been motivated to seek out references such as Grabelsky for example implementations showing the entire format of packets in an IPSec system. *Id.* at 38 (citing Ex. 1002 ¶ 104).

e. Unique Identity and Destination Address

Petitioner argues that RFC3104 teaches "wherein the unique identity and the destination address are capable of being used by the intermediate computer to find an address to a recipient computer," as recited in claim 1. Pet. 43. More specifically, Petitioner argues that RFC3104 teaches "that when 'IP[S]ec packets from Y destined for X arrive at RSIP server N,' '[t]hey are demultiplexed based on the following minimum tuple of demultiplexing fields:'" "protocol (50 or 51)," "SPI," and "destination IP address." *Id.* (quoting Ex. 1004, 5). "This minimum tuple of demultiplexing fields, which includes the 'destination IP address' of RSIP server N, is part of a 'unique identity' of the IPSec packet received from Y," according to Petitioner. *Id.* (citing Ex. 1002 ¶ 113). According to Petitioner, "RFC3104 then teaches, '[i]f N is able to find a *matching mapping*, it tunnels the packet to X according to the tunneling mode in effect.'" *Id.* (citing Ex. 1004, 5). Petitioner argues that one of ordinary skill in the art "would have understood that the mapping between the 'minimum tuple of demultiplexing fields' (which includes the 'destination IP address') and host X is '*used by the*

intermediate computer to find an address to a recipient computer.'" *Id.* (citing Ex. 1002 ¶ 113). In other words, "the mapping is used to look up destination host X and its address so that RSIP server N can forward the packet to X," according to Petitioner. *Id.*

f. Send the Secure Message

Petitioner argues that RFC3104 teaches that "the computer [is] configured to send the secure message to the intermediate computer for forwarding of the encrypted data payload to the recipient computer," as recited in claim 1. *Id.* at 44. More specifically, Petitioner argues that an IPSec SA "('*secure connection*') is established from Y to X." *Id.* (citing Ex. 1004, 5). "Host Y then uses this established SA to form and send packets to X via RSIP server N," according to Petitioner. *Id.* Petitioner argues that "[w]hen 'IP[S]ec packets from Y destined for X arrive at RSIP server N . . . [t]hey are demultiplexed,' and '[i]f N is able to find a *matching mapping*, it tunnels the packet to X according to the tunneling mode in effect.'" *Id.* (citing Ex. 1004, 5; Ex. 1002 ¶¶ 114–115).

g. Set Up a Secure Connection

Petitioner argues that RFC3104 teaches that "the computer [is] configured to set up a secure connection using a key exchange protocol," as recited in claim 1. *Id.* at 44–45. According to Petitioner, RFC3104 teaches that "[t]he IPSec SA from Y to X is established through use of an Internet Key Exchange (IKE) protocol, . . . 'namely, *Quick Mode in IKE*.'" *Id.* (quoting Ex. 1004, 5). Petitioner argues that one of ordinary skill in the art "would have understood that the use of 'Quick Mode in IKE' involves a negotiation and exchange of keys (between X and Y in this case), e.g.,

Diffie-Hellman key information." *Id.* at 45 (citing Ex. 1002 ¶ 117 (citing Ex. 1018, 16–19)).

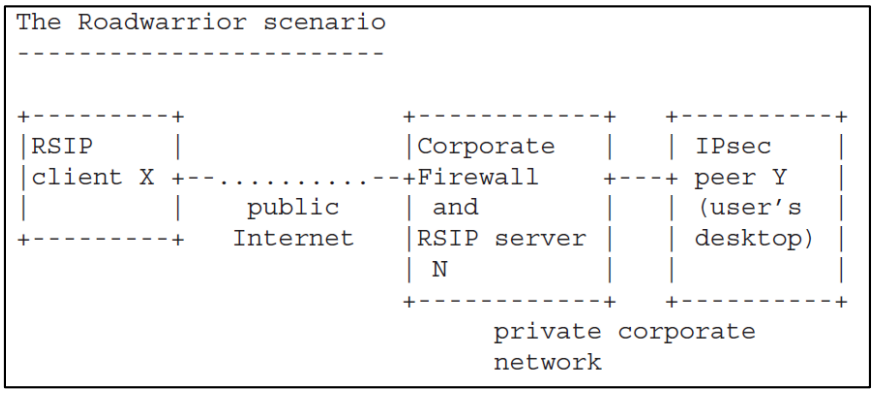
h. Our Analysis

After reviewing Petitioner's arguments and evidence regarding the limitations identified above, which are not addressed by Patent Owner (*see generally* PO Resp.), we are persuaded that Petitioner demonstrates by a preponderance of the evidence that the combination of RFC3104 and Grabelsky teaches the above identified undisputed limitations.

2. Mobile Computer

We agree with Petitioner that RFC3104 teaches that "wherein the computer is a mobile computer in that the address of the mobile computer changes," as recited in claim 1. Pet. 31–35. In particular, RFC3104 discloses specific scenarios in which a host is a mobile computer. Ex. 1004, 3, 16; Pet. 32. For example, RFC3104 discloses the "Roadwarrior scenario." Ex. 1004, 3, 16; Pet. 32–33.

In the "Roadwarrior scenario," "a remote user with a laptop gains access to the Internet," and "wants to access its corporation['s] private network." Ex. 1004, 16. RFC3104 provides a diagram, shown below, of this scenario. *Id.*



The Roadwarrior scenario diagram, shown above, illustrates an example application of RFC3104's teachings. *Id.* As illustrated, RSIP client X (laptop) is shown as connected to the public Internet, with host Y part of a private corporate network. Ex. 1004, 16; Pet. 33. We agree with Petitioner and find that "[b]ecause the user with the laptop is on the road, . . . [one of ordinary skill in the art] would have understood that the laptop would change its point of attachment and its address when connecting to the Internet from different locations." Ex. 1002 ¶ 94; Pet. 33–34; *see also* Ex. 2003 ¶ 105 ("A POSITA would understand that as a computer changes networks it will change IP addresses."). Put differently, the laptop is physically mobile and the term "[r]oadwarrior" at least suggests that the remote user is on the road, changing networks frequently. Ex. 1002 ¶ 94; *see also* Ex. 2003 ¶ 105 ("A POSITA would understand that a businessperson on the road with a laptop can be expected to connect to different networks and have different fixed IP addresses at different points in time."). Hence, we find that RSIP client X, in the Roadwarrior scenario, is a mobile computer (i.e., a computer that is capable of moving between networks). Ex. 1004, 16; Ex. 1002 ¶ 94.

Moreover, we find that client X being a mobile computer connected to the public Internet in the Roadwarrior scenario teaches that host Y in the Model topology also is a mobile computer, as host Y is connected to the public Internet. *Compare* Ex. 1004, 2–3, *with id.* at 16; Ex. 1002 ¶ 93 (opining that at least the computer connected to the public Internet would be a mobile computer).

Regardless, RFC3104 teaches for the Roadwarrior scenario "that RSIP server N 'would use RSIP to selectively enable IP[S]ec traffic between

internal and external systems,' thus allowing packets to be sent from RSIP client X to host Y, and vice versa." Pet. 33; Ex. 1004, 16; Ex. 1002 ¶ 93. RFC3104 additionally teaches that the Roadwarrior "scenario could also be reversed in order to allow an internal system (Y) to initiate and establish an IP[S]ec session with an external IP[S]ec peer (X)." Ex. 1004, 16; Pet 33. This reversed Roadwarrior scenario would mirror the Model topology in that the internal (i.e., private corporate network) system would initiate and establish an IPSec session with an external (public Internet) IPSec peer. Ex. 1004, 2–3, 16. In the context of the reversed Roadwarrior scenario, this teaches a specific scenario in which the external IPSec peer is a mobile computer (i.e., a laptop of a remote user on the road), which further supports that host Y in the Model topology is (or it would be obvious to be) a mobile computer. *Id.* Accordingly, we agree with Petitioner and find that one of ordinary skill in the art "would have understood that either RFC3104's host Y or X could be (and often would be) a '*mobile computer*.'" Ex. 1002 ¶ 92 (emphasis added); Pet. 32.

Alternatively, we are persuaded that one of ordinary skill in the art would have found it obvious to have host Y in the Model topology be a mobile computer in view of the Roadwarrior scenario teaching a mobile computer. Ex. 1004, 2–3, 16; Ex. 1002 ¶¶ 91–94; *see also In re Preda*, 401 F.2d 825, 826 (CCPA 1968) ("[I]t is proper to take into account not only specific teachings of the references but also the inferences which one skilled in the art would reasonably be expected to draw therefrom."); *KSR*, 550 U.S. at 417 ("If a person of ordinary skill can implement a predictable variation, § 103 likely bars its patentability.").

We are not persuaded by Patent Owner's argument that "Dr. Goldschlag's testimony should be given little to no weight because it is conclusory, and it fails to provide reasoning linked to an articulated factual basis to support the assertion that RSIP Host X must be a mobile computer because Host X is connected to the public Internet." PO Resp. 37 (citing Ex. 1002 ¶94). Rather, we find that the "public" nature of public Internet factually supports Dr. Goldschlag's testimony that RSIP client X would be a mobile computer, as members of the public would access the public Internet and establish connections from varying public locations. Moreover, we find Dr. Goldschlag's testimony (paragraph 93) states "[i]n this case" and "as discussed in this scenario," which refers back to at least paragraph 92, and he there provides a further rational basis (e.g., that its the Roadwarrior scenario's laptop (a moveable device) which is connected to the public Internet) for at least his opinions in paragraphs 93 and 94 of his Declaration. Ex. 1002 ¶¶ 92–94. We also find inapposite Patent Owner's argument that "[a] computer can be connected to the public Internet using a fixed IP address." PO Resp. 35; *see also id.* at 35–36 (citing Ex. 2003 ¶ 112). Patent Owner does not address that different fixed addresses would be used if a member of the public establishes connections from varying public locations. *See* Ex. 1002 ¶ 94; Ex. 2003 ¶ 105. And, as the '502 patent's Specification teaches, connections can be made at every newly visited site. Ex. 2002, 4:23–25, 4:51–52.

Lastly,[10] we find that Patent Owner's remaining arguments for this limitation are premised on either its (i) proposed construction (i.e., a mobile computer is "a computer that moves from one network to another as opposed to a computer that is only capable of a static secure connection"), which we do not adopt, or (ii) inapposite argument that the mobile computer needs to maintain the same secure connection. *See* PO Resp. 26–54. Thus, we find these arguments unavailing. Likewise, Dr. Borella's declaration testimony is not helpful to our analysis as his "declaration employs the assumption that the 'mobile computer' recited in the claims moves from one network to another," which is contrary to our construction, as we discuss above. Ex. 2010 ¶ 42; *supra* Section IV(B) (construing mobile computer).

In summary, we find that RFC3104 teaches "wherein the computer is a mobile computer in that the address of the mobile computer changes," in accordance with claim 1.

3. Alleged Erroneous Obviousness Standard

Patent Owner argues that Petitioner's expert, Dr. Goldschlag, applies an incorrect obviousness standard. PO Sur-Reply 11–13. In particular, Patent Owner argues that Dr. Goldschlag opines on "how the prior art references could have been combined," rather than opining that one of ordinary skill in the art "*would* have an apparent reason to combine and/or modify the prior art as proposed." *Id.* at 11–12 (citing Ex. 1002 ¶ 25; Ex. 1022 ¶ 2) (emphasis added). We find this argument unavailing.

[10] We need not, and thus do not, reach whether Petitioner's arguments for this limitation in its Reply (Pet. Reply 9–14) are new arguments, as Patent Owner argues in its Sur-Reply (PO Sur-Reply 13–25), because we do not rely on them, but instead, we rely on Petitioner's arguments, and citations to the record evidence, from the Petition.

This is a new argument, at least with respect to Dr. Goldschlag's declaration submitted with the Petition (Ex. 1002), and should have been raised in Patent Owner's Response, if at all. *See* Paper 8, 7; Consolidated Practice Guide 74 (citing 37 C.F.R. § 42.23). Regardless, Dr. Goldschlag's testimony upon which we rely for the obviousness grounds states that one of ordinary skill in the art "would" (rather than "could") have found it obvious to combine the relevant teachings. *E.g.*, Ex. 1002 ¶ 74, 80–84; Pet. 23–28.

In addition, we find unavailing Patent Owner's argument that "Dr. Goldschlag's obviousness test also omits the requirement that he must demonstrate that a person of ordinary skill would have a reasonable expectation of success that the proposed combination and/or modification of the prior art would operate for its intended purpose." PO Sur-Reply 13. This argument is untethered to any specific testimony of Dr. Goldschlag, and thus fails to inform us properly of the scope of this argument. Nonetheless, we find Dr. Goldschlag's testimony that we rely on herein sufficiently supported by the factual record for the weight we afford it. *E.g.*, Ex. 1002 ¶ 74, 80–84. For example, Dr. Goldschlag testifies that "RFC3104 already discloses sending IPSec packets from host Y to RSIP client X via RSIP server N," and "would have informed [one of ordinary skill in the art] of standard formatting for those packets, including parameters contained in the IP and IP[S]ec protocol headers." *Id.* ¶ 80. Dr. Goldschlag further testifies that the combination "would amount to merely combining known elements to yield predictable results." *Id.* Nor are we persuaded by Patent Owner's argument that Dr. Goldschlag's original declaration is "replete with conclusory reasoning applying his hindsight-biased framework to find obviousness based on his 'could have' standard." PO Sur-Reply 12

(citations omitted). For example, Dr. Goldschlag testifies that one of ordinary skill in the art "would have understood that either RFC3104's host Y or X could be (*and often would be*) a mobile computer." Ex. 1002 ¶ 92 (emphasis added). Thus, Dr. Goldschlag clearly testifies that one of ordinary skill in the art would have understood that host Y or X often *would* be a mobile computer. *Id.*

4. Summary

In summary, based on the arguments and evidence of record discussed above, we find that Petitioner has demonstrated by a preponderance of the evidence that claim 1 is unpatentable under 35 U.S.C. § 103(a) based on RFC3104 and Grabelsky.

D. Challenged Claims 2–6

Petitioner argues, with specific cites to the references and Dr. Goldschlag's testimony, that the combination of RFC3104 and Grabelsky teaches the limitations recited in claims 2–6. Pet. 45–61.

Patent Owner did not separately address Petitioner's arguments directed to these claims. PO Resp. 59 (arguing that "[d]ependent claims 2–6 are patentable over the combination of RFC3104 and Grabelsky for at least the reasons set forth above . . . for independent claim 1"); PO Sur-Reply 26.

Based on the evidence and arguments presented in the Petition, we find that Petitioner has demonstrated by a preponderance of the evidence that claims 2–6 would have been obvious to one of ordinary skill in the art over the combined teachings of RFC3104 and Grabelsky.

E. Challenged Claims 7–9

Claim 7 depends from independent claim 1, and recites "[t]he computer of claim 1, wherein the computer is configured to send a signaling

message to the intermediate computer when the computer changes its address such that the intermediate computer can know that the address of the computer is changed." Ex. 2002, 23:11–15. Petitioner argues that RFC3104 teaches this limitation. Pet. 51–53; Pet. Reply 19–22. We disagree.

Petitioner argues that RFC3104's ASSIGN_REQUEST_RSIPSEC message acts as the signaling message. Pet. 53 (citing Ex. 1004, 7; Ex. 1002 ¶ 133). More specifically, Petitioner argues that a ASSIGN_REQUEST_RSIPSEC message requests IPSec parameter assignments, and once assigned, "an SA can be established between the RSIP client and its peer." *Id.* at 52 (citing Ex. 1004, 5; Ex. 1002 ¶ 131). Petitioner argues that "[a]t this point, [one of ordinary skill in the art] would have understood that a mapping of 'demultiplexing fields' to the network address of the RSIP client would need to be created." *Id.* (citing Ex. 1004, 5; Ex. 1002 ¶ 131); Pet. Reply 17. "Thus, when the RSIP client moves to a new address, the 'ASSIGN_REQUEST_RSIPSEC message' causes '*a signaling message*' to be sent '*to the intermediate computer* [i.e., RSIP server N] . . . *such that the intermediate computer can know that the address of the computer is changed*,'" according to Petitioner. Pet. 53 (citing Ex. 1004, 7; Ex. 1004 ¶ 133).

We are not persuaded by Petitioner's arguments, but rather agree with Patent Owner that "the ASSIGN_REQUEST_RSIPSEC message is used to establish an RSIP-IPSec session, not to signal address changes of Host X or Host Y." PO Resp. 56; Ex. 1004, 5, 7. At most, a ASSIGN_REQUEST_RSIPSEC message provides for a new SA to be established between the RSIP client and its peer when the computer changes its address. Ex. 1004, 5, 7; Ex. 1002 ¶ 131. Claim 7 requires, however, "a

signaling message . . . such that the intermediate computer *can know that the address of the computer is changed*." Ex. 2002, 23:11–15. Petitioner does not show that the intermediate computer "knows" that the address is changed, as required by the claim language. *In re Hiniker Co.*, 150 F.3d 1362, 1369 (Fed. Cir. 1998) ("[T]he name of the game is the claim."). In other words, Petitioner does not show that the intermediate computer knows that the address is changed, as opposed to simply having a new SA being established. Ex. 1004, 5, 7; Ex. 1002 ¶ 131.

Accordingly, Petitioner has not demonstrated by a preponderance of the evidence that claim 7 of the '502 patent would have been obvious to one of ordinary skill in the art in view of RFC3104 and Grabelsky. In addition, claims 8 and 9 depend, directly or indirectly, from claim 7 and incorporate claim 7's limitations. Ex. 2002, 23:16–19. Petitioner's showings for claims 8 and 9 fail to remedy the deficiency in Petitioner's showing for claim 7, discussed above. Pet. 53–54; Pet. Reply 18–21. Accordingly, Petitioner has not demonstrated by a preponderance of the evidence that claims 8 and 9 of the '502 patent would have been obvious to one of ordinary skill in the art in view of RFC3104 and Grabelsky.

VII. ALLEGED OBVIOUSNESS OVER RFC3104, GRABELSKY, AND WAGNER

Petitioner argues, with specific cites to the references and Dr. Goldschlag's testimony, that the combination of RFC3104, Grabelsky, and Wagner renders claim 10 obvious. Pet. 54–58.

Patent Owner did not separately address Petitioner's arguments directed to this claim. PO Resp. 59 (arguing that "[c]laim 10 is patentable

over the cited prior art for at least the reasons set forth for claim 1 addressed for" the RFC3104 and Grabelsky ground); PO Sur-Reply 26.

Based on the evidence and arguments presented in the Petition, we determine that Petitioner has demonstrated by a preponderance of the evidence that claim 10 would have been obvious over the combined teachings of RFC3104, Grabelsky, and Wagner.

VIII. CONSTITUTIONAL CHALLENGE

Patent Owner argues that Administrative Patent Judges are unconstitutionally appointed principal officers, and that the decision in *Arthrex, Inc. v. Smith & Nephew, Inc.*, 941 F.3d 1320, 1337 (Fed. Cir. 2019), *cert. granted sub nom. United States v. Arthrex, Inc.*, 2020 WL 6037206 (Oct. 13, 2020) was inadequate to cure the Constitutional violation. PO Resp. 59–60. We note that Patent Owner's constitutional challenge was addressed by the Federal Circuit's *Arthrex* decision. *Arthrex*, 941 F.3d at 1337 ("This as-applied severance . . . cures the constitutional violation."); *see also Arthrex, Inc. v. Smith & Nephew, Inc.*, 953 F.3d 760, 764 (Fed. Cir. 2020) (en banc) (Moore, J., concurring in denial of rehearing) ("Because the APJs were constitutionally appointed as of the implementation of the severance, *inter partes* review decisions going forward were no longer rendered by unconstitutional panels."). Accordingly, we do not consider this issue any further.

Patent Owner also argues that "the challenged patent was applied for and published before enactment of the America Invents Act (AIA)," and that "[s]ubjecting such patents to AIA proceedings is an unconstitutional taking of property without just compensation and an unconstitutional deprivation of property without due process." PO Resp. at 60 (citation omitted). With

regard to the Takings and Due Process Clause challenges, we note that challenges to retroactive application of IPRs to pre-AIA patents have been addressed by the Federal Circuit in *Celgene Corp. v. Peter*, 931 F.3d 1342, 1357–1363 (Fed. Cir. 2019), *cert. denied* 2020 WL 3405867 (June 22, 2020) (Takings Clause) and *Sound View Innovations, LLC v. Hulu, LLC*, Nos. 2019-1865, 2019-1867, 2020 WL 3583556, *3 (Fed. Cir. July 2, 2020) (non-precedential) (Due Process Clause). Accordingly, we do not consider this issue any further.

IX. CONCLUSION[11]

Based on the full record before us, we determine that Petitioner has demonstrated by a preponderance of the evidence that (i) claims 1–6 of the '502 patent are unpatentable under 35 U.S.C. § 103(a) in view of RFC3104 and Grabelsky and (ii) claim 10 is unpatentable under 35 U.S.C. § 103(a) in view of RFC3104, Grabelsky, and Wagner. We also determine that Petitioner has not demonstrated by a preponderance of the evidence that claims 7–9 of the '502 patent are unpatentable under 35 U.S.C. § 103(a) in view of RFC3104 and Grabelsky.

[11] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

Claim(s)	35 U.S.C §	Reference(s) /Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–9	103(a)	RFC3104, Grabelsky	1–6	7–9
10	103(a)	RFC3104, Grabelsky, Wagner	10	
Overall Outcome			1–6, 10	7–9

X. ORDER

In consideration of the foregoing, it is hereby

ORDERED that, pursuant to 35 U.S.C. § 314(a), Petitioner has shown by a preponderance of the evidence that claims 1–6 and 10 of the '502 patent are unpatentable;

FURTHER ORDERED that Petitioner has not shown by a preponderance of the evidence that claims 7–9 of the '502 patent are unpatentable; and

FURTHER ORDERED that parties to the proceeding seeking judicial review of this Final Written Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2019-00824
Patent 9,712,502 B2

PETITIONER:

Michael D. Specht
Daniel S. Block
Steven M. Pappas
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
mspecht-ptab@sternekessler.com
dblock-ptab@sternekessler.com
spappas-PTAB@sternekessler.com

PATENT OWNER:

James T. Carmichael
Stephen T. Schreiner
CARMICHAEL IP LAW, PLLC
jim@carmichaelip.com
schreiner@carmichaelip.com

Kenneth J. Weatherwax
Patrick Maloney
Jason C. Linger
LOWENSTEIN & WEATHERWAX LLP
weatherwax@lowensteinweatherwax.com
maloney@lowensteinweatherwax.com
linger@lowensteinweatherwax.com

Christopher J. Lee
Richard B. Megley
Brian E. Haan
Ashley E. LaValley
LEE SHEIKH MEGLEY & HAAN LLC
clee@leesheikh.com
rmegley@leesheikh.com
bhaan@leesheikh.com
alavalley@leesheikh.com